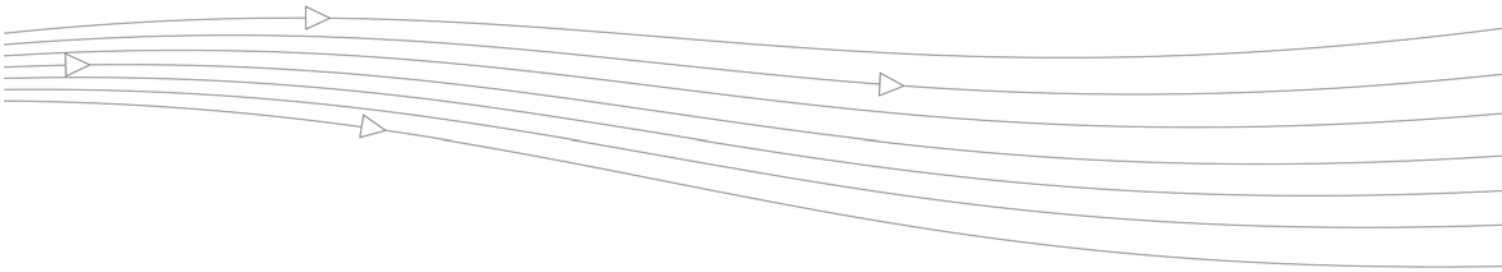


SonicWALL® Anti-Spam Desktop User Guide

Version 6.2

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Part Number: 232-001812-00 Rev A

SonicWALL Anti-Spam Desktop Client

User Guide for Windows

v6.2

© 2009 SonicWALL, Inc. All rights reserved. SonicWALL is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

About SonicWALL Anti-Spam Desktop 1
How SonicWALL Anti-Spam Desktop Works. 2
Features and Benefits. 2
Installing and Getting Started 4
Supported Platforms 4
Registering and Licensing 4
Support 5
Downloading and Installing SonicWALL Anti-Spam Desktop 6
Types of Deployments 6
In-House Microsoft Exchange Server and SonicWALL Anti-Spam Desktop 6
Hosted Email and SonicWALL Anti-Spam Desktop 7
SonicWALL Email Security and SonicWALL Anti-Spam Desktop 7
Using SonicWALL Anti-Spam Desktop. 8
Configuring SonicWALL Anti-Spam Desktop 11
SonicWALL Options 11
SonicWALL System Tray 13
People 14
Companies 15
Lists. 17
Messages 18
Challenges 19
Settings 21
Reports 23
Troubleshooting 23

About SonicWALL Anti-Spam Desktop

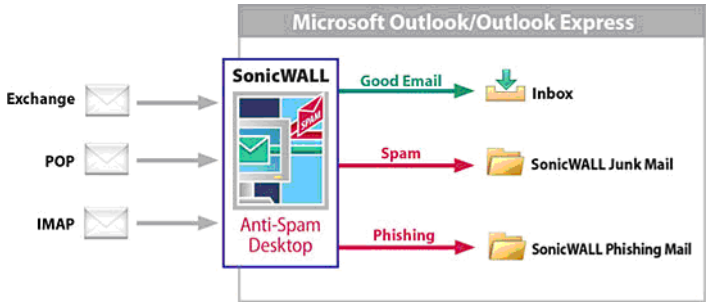
SonicWALL Anti-Spam Desktop makes email good again. Before spammers invaded, the email you received was wanted email. No one sent you unwanted messages. Unfortunately, spam has increased exponentially over the last 10 years and shows no signs of stopping. In addition to clogging your Inbox, email today includes phishing, viruses and other malicious threats.

SonicWALL Anti-Spam Desktop is an innovative solution that keeps spam and phishing out of your Inbox. SonicWALL Anti-Spam Desktop delivers client-based anti-spam and anti-phishing protection for Microsoft Outlook, Outlook Express, or Windows Mail email clients on Windows-based desktops or laptops. With SonicWALL Anti-Spam Desktop, email once again becomes a tool to enhance productivity - instead of a source of user frustration and administrative dread. SonicWALL has engineered Anti-Spam Desktop to deliver the same world class email protection for individual clients as SonicWALL's award-winning enterprise appliance and software solutions deliver for enterprises.

Installation is easy. Once you download and install SonicWALL Anti-Spam Desktop, it instantly monitors your email. Good email goes to your Inbox; spam and phishing email is stored in your SonicWALL Junk Mail folder. Once messages are placed in your SonicWALL Junk Mail folder, you can choose to review junked messages to see if there is anything you want.

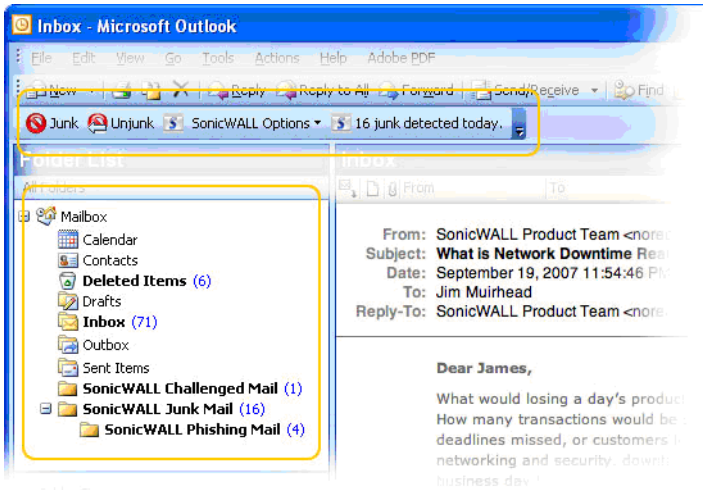
SonicWALL Anti-Spam Desktop integrates with Outlook and Outlook Express, and can filter mail from POP and Microsoft Exchange accounts. It can also be used with Hotmail and IMAP accounts, when used with Outlook Express.

When SonicWALL Anti-Spam Desktop is installed on a Microsoft Windows system it acts as a plug-in to Outlook, Outlook Express, or Windows Mail. Anti-Spam Desktop evaluates email arriving from Exchange, POP, or IMAP to the Outlook, Outlook Express, or Windows Mail client, and prevents spam and phishing email from reaching the Inbox.



How SonicWALL Anti-Spam Desktop Works

Once installed, SonicWALL Anti-Spam Desktop starts whenever your email client is started. Anti-Spam Desktop evaluates email as it arrives, placing spam email in the Junk Mail folder, phishing email in the Phishing Mail folder, and legitimate email in the Inbox. With the Challenges option, challenged email is placed in the *Challenged Mail* folder.



If a spam message is delivered to the Inbox, highlight the message and click **Junk** to remove it from the Inbox. This also adds the sender to a blocked list so that future email from this sender is blocked as spam. If a legitimate email be placed in the Junk Mail folder unintentionally, highlight the message and click **Unjunk**. This action also adds the sender to an allowed list so that future email from that person is delivered correctly.

Features and Benefits

SonicWALL Anti-Sam Desktop installs on a Windows-based desktop or laptop in minutes to immediately begin protecting Outlook, Outlook Express, or Windows Mail Inboxes from spam and phishing email. There are no rules to create and no lists to populate. With continued use, SonicWALL Anti-Spam Desktop learns about unwanted email types, to continuously improve Inbox protection.

Real-Time Protection

To stay up-to-date on evolving spam, phishing and malware attacks, all SonicWALL Email Security solutions interact in real-time with the SonicWALL GRID Network. With unparalleled accuracy, the SonicWALL GRID Network is a collaborative effort that gathers, analyzes, and confirms cross-vector threat information from a distributed network of millions of business-oriented sources around the world. After evaluating hundreds of millions of email messages each day, threat protection information is then distributed securely, anonymously, and in real time to improve the overall effectiveness of all SonicWALL security solutions.

For each email message, the GRID Network determines the reputation of the sender, content, links, images attachments, and more. The GRID Network's collaborative filtering process enables SonicWALL Anti-Spam Desktop to deliver highly accurate, fully self-correcting, and up-to-date protection.

Powerful Bayesian Filtering

SonicWALL Anti-Spam Desktop stops spam with its unique Adversarial Bayesian Filtering Engine. Bayesian filtering examines the content of an email message to determine if it is spam. Unlike many spam filters, SonicWALL Anti-Spam Desktop also considers hundreds of other email attributes, detecting even the most subtle spammer tricks.

Unique Anti-Phishing Protection

SonicWALL Anti-Spam Desktop has the industry's only Bayesian Phishing Engine. This allows SonicWALL to detect phishing email with unsurpassed accuracy. Dangerous email messages are placed in a designated Phishing folder, which dramatically reduces the risk of having financial, personal or proprietary information lost through an email-based phishing attack.

Easy-To-Manage Allowed And Blocked Lists

Allowed and Blocked lists allow you to personalize SonicWALL Anti-Spam Desktop to meet your specific spam blocking needs. SonicWALL Anti-Spam Desktop automatically creates and updates a People (email address) Allowed and Blocked List. You can also update these lists manually. In addition, SonicWALL Anti-Spam Desktop allows each user to create and maintain a Company (domain name) Allowed and Block list and a Mailing List Allowed List.

Flexible Controls

Once installed, SonicWALL Anti-Spam Desktop begins blocking spam and phishing email immediately. Users have the power to change the aggressiveness of the spam detection settings based on the content of the message. For example, a user can be more aggressive in blocking email with obscene language, but less aggressive in blocking email containing advertisements. Users can even choose to block or allow messages based on language. This flexibility lets users fine-tune SonicWALL Anti-Spam Desktop.

Challenge-Response Ready

SonicWALL Anti-Spam Desktop can challenge none, some, or all of the email messages received from unknown senders. Challenges can be text or a visual image, and users can customize the challenge message.

Connection To All SonicWALL Email Security Solutions

When SonicWALL Anti-Spam Desktop is running on a desktop or laptop, it determines whether there is an upstream active copy of a SonicWALL Email Security appliance or software solution. If so, SonicWALL Anti-Spam Desktop attempts to “push” its People Allowed and Block Lists to the SonicWALL Email Security solution, assuming that appropriate login credentials are provided and you are allowed to update these lists on the SonicWALL Email Security system. Once set up, this connectivity allows the user to use the **Junk** and **Unjunk** buttons in SonicWALL Anti-Spam Desktop and have the Allowed and Blocked List automatically updated on the SonicWALL Email Security solution.

SonicWALL Email Security is not required for Anti-Spam Desktop to operate, and vice-versa.

Many Other Features

- **Multiple Inbox Support**—The Outlook version of Anti-Spam Desktop can scan one or more different inboxes.
- **Scan Folder Option**—Users can re-scan their inbox or any other folder by simply selecting that folder and using the Scan Selected Folder option
- **Automatic Re-scanning**—The SonicWALL GRID Network is always discovering new spam, phishing attacks and malware. This option removes any newly discovered spam from the inbox.
- **Wireless Device Support**—Email received by a desktop or laptop and forwarded to a wireless device can have spam and phishing removed before it is sent out.
- **Language Blocking**—You can choose to block email in languages you don't want to receive.
- **Spam Blocking Aggressiveness Sliders**—Provides slider controls to determine how aggressively to block different flavors of spam
- **Automatic Junk Deletion**—Lets you set how long junk is kept before it is moved to the Deleted folder.
- **Email Server Authentication Support**—Enables use of email servers that require authentication

- **Outlook and Outlook Express**—Seamless integration with Outlook and Outlook Express.
- **Windows Mail** — Seamless integration with Windows Mail.
- **Automatic Setup**—SonicWALL learns those people with whom you exchange email and those that you block. It adapts to your email characteristics, without complicated rules or settings.

Installing and Getting Started

To complete the installation of SonicWALL Anti-Spam Desktop, you must have administrative permissions on the system you are installing to.

Supported Platforms

SonicWALL currently supports the following platform / email client combinations for Anti-Spam Desktop. While Anti-Spam Desktop may operate on other combinations, such combinations are not officially supported.

Operating System	Mail Clients		
Windows 7	Outlook 2007	Outlook 2003	
Vista (32 & 64-bit)	Outlook 2007	Outlook 2003	Windows Mail
Windows XP	Outlook 2007	Outlook 2003	Outlook Express 6.0

Registering and Licensing

There are three ways to get a copy of SonicWALL Anti-Spam Desktop. Once you download your copy by clicking a link, you must enter your License Key to verify your purchase.

From your partner	From mysonicwall.com	From Digital River
If your license for SonicWALL Anti-Spam desktop is provided by a partner, request the download link and license key from your partner.	Log in to your mysonicwall.com account and visit the Download section. Select the version of Anti-Spam Desktop you want and click the link to start the download.	If you have purchased an individual license for SonicWALL Anti-Spam Desktop from Digital River, the link and license key will be sent to you using the email address you used during purchase.

A License Key allows the SonicWALL Anti-Spam Desktop software to operate for the period of time for which you have purchased a subscription. A License Key is similar in form to the following: `aaaa-bbbb-cccc-dddd-eeee-ffff`.

If youSonicWALL Anti-Spam Desktop software says it is expired, there are two possible reasons:

- The License key has expired and the software must be renewed. When you purchase a renewal you are provided with a new License Key, which replaces the existing License Key.
- You have not entered a valid License Key. Even if you have purchased the software and obtained a License Key, the key must still be entered into the product itself.

If you have a 30-day trial copy , you can convert it to a licensed copy by entering a valid License Key.

Entering Your License Key

Your license includes dynamic spam signature file updates, product upgrades, and email support for one, two, or three years. (Note: Users who purchase SonicWALL Anti-Spam Desktop from the web receive their license key via email.) Each year thereafter, you can choose to receive an additional year of the above services by paying an annual maintenance fee.

▶ **To enter your license key**

1. Click **Buy Now** from the Windows System Tray or the Toolbar menu:

2. Enter the license key to SonicWALL Anti-Spam Desktop in the space provided. License keys are a sequence of 24 letters in groups of four, and look like: aaaa-bbbb-cccc-dddd-eeee-ffff.

NOTE: These keys are case sensitive.

Once you have entered the key, you have completed SonicWALL Anti-Spam Desktop activation.

When Your SonicWALL Anti-Spam Desktop Trial Expires

Before entering your license key, your version of SonicWALL Anti-Spam Desktop runs as a free trial for 30 days. After 30 days, SonicWALL displays an alert that it is time to purchase SonicWALL Anti-Spam Desktop.

Support

SonicWALL Anti-Spam Desktop is a simple product that has been installed and is operating on millions of desktop and laptop systems worldwide. Most problems can be quickly resolved by following these steps:

a. Use the online help.

b. Go to the SonicWALL Anti-Spam Desktop support Web page on www.sonicwall.com. You'll have access to release and technical notes, and the support knowledge base portal.

c. Contact your SonicWALL reseller, who is in the best position to answer questions regarding licensing, renewals, purchases, and so on. They also have the "Virtual Serial Number" and the contact information needed to contact SonicWALL Technical Support.

d. Ask your reseller to use the Web form on the Support page to send an email message to SonicWALL Technical support at ASDSupport@sonicwall.com.

The Virtual Serial Number is created when someone registers a purchase of SonicWALL Anti-Spam Desktop in their mysonicwall.com account. The Virtual Serial Number is needed to contact SonicWALL Technical Support to ensure that only people who have paid for the SonicWALL Anti-Spam Desktop receive support.

All SonicWALL Email Security products are available from any SonicWALL reseller through standard SonicWALL distribution channels. SonicWALL resellers can purchase the software from distribution for end users. SonicWALL Anti-Spam Desktop is available in 5, 10 and 25 packs in 1, 2 or 3 year subscriptions that must be renewed to stay up to date. Renewals are also purchased from SonicWALL resellers. The price of the software is set by the SonicWALL reseller.

Individual users can also purchase SonicWALL Anti-Spam Desktop through our third-party fulfillment agency, Digital River.

MailFrontier Desktop Customers

SonicWALL Anti-Spam Desktop is a new version of MailFrontier Desktop that has been branded as a SonicWALL product. SonicWALL Anti-Spam Desktop replaces MailFrontier Desktop.

If your subscription of MailFrontier Desktop is current, you will be automatically upgraded to SonicWALL Anti-Spam Desktop.

If your subscription for MailFrontier Desktop has expired, you can click **Buy Now** in the product for instructions on renewing your subscription.

Downloading and Installing SonicWALL Anti-Spam Desktop

Downloading and installing SonicWALL Anti-Spam Desktop takes only a few minutes.

- Click the link provided to start the download process. Depending on your browser settings, you may be asked to approve the download. The size of the downloaded file is 7-8 MB.
- Once the download is complete, open the downloaded file and approve running it. The installation process begins, and will take 5 minutes or less.

Anti-Spam Desktop will always start automatically, and you can access the settings using the SonicWALL logo located in the system tray and in your mail application tool bar.

NOTE:

- You do not need to configure SonicWALL Anti-Spam Desktop. It automatically adapts to your preferences. On first use, Anti-Spam Desktop scans your Sent Items folder to include your known recipients in your Allowed list. When you choose to junk a message, SonicWALL Anti-Spam Desktop puts the sender's email address in your Blocked List.

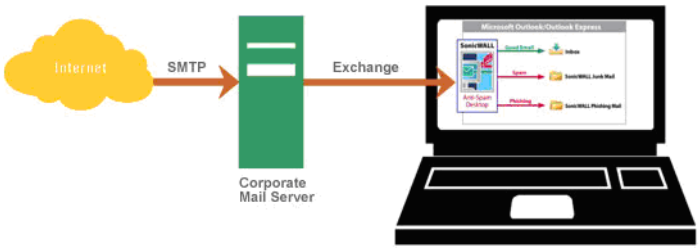
Once you have installed SonicWALL Anti-Spam Desktop, the SonicWALL logo appears in the system tray and in your mail application tool bar.

Types of Deployments

SonicWALL Anti-Spam Desktop can be deployed in many ways to prevent spam and phishing attacks. Anti-Spam Desktop protects numerous Outlook, Outlook Express, and Windows Mail clients running on Windows 7, Windows Vista and Windows XP platforms. The following section examines three typical deployment configurations, using in-house Exchange, hosted email and SonicWALL Email Security.

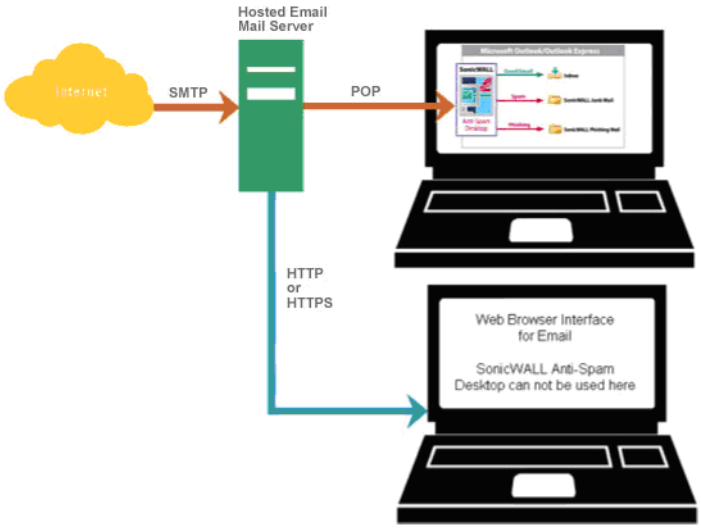
In-House Microsoft Exchange Server and SonicWALL Anti-Spam Desktop

In this scenario, email is received from the Internet and each user connects to the in-house email Microsoft Exchange email server. Email is downloaded to the Outlook or Outlook Express client on a regular basis and is filtered for spam and phishing by SonicWALL Anti-Spam Desktop. There is no requirement for the Email Server to reside in-house as long as the client can reach the server to retrieve email. Alternatively, the Outlook, Outlook Express, or Windows Mail client may use POP or IMAP to pull down received email from a separate email server.



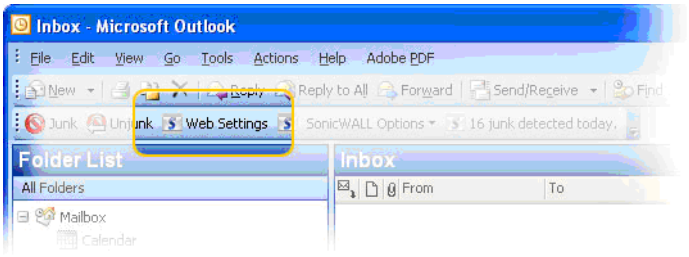
Hosted Email and SonicWALL Anti-Spam Desktop

For many organizations, an ISP or email hosting company receives the email and stores it until it is accessed by individual users. In this scenario, Anti-Spam Desktop can be deployed to protect mail clients accessed via POP. This solution is not used for email accessed by the client via HTTP or HTTPS.

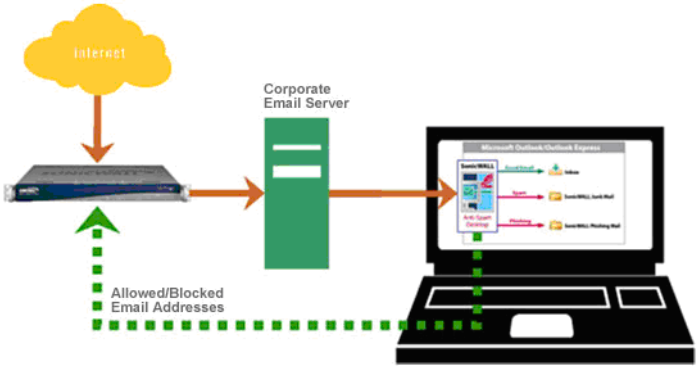


SonicWALL Email Security and SonicWALL Anti-Spam Desktop

If Anti-Spam Desktop detects an upstream SonicWALL Email Security device (appliance or software), it displays a Web Settings menu on the Toolbar.



In this scenario, Allowed and Block List information is copied upstream from SonicWALL Anti-Spam Desktop to SonicWALL Email Security. In this configuration, each user has two Junk Mail Boxes: one on the Email Security System and one on the Desktop client.



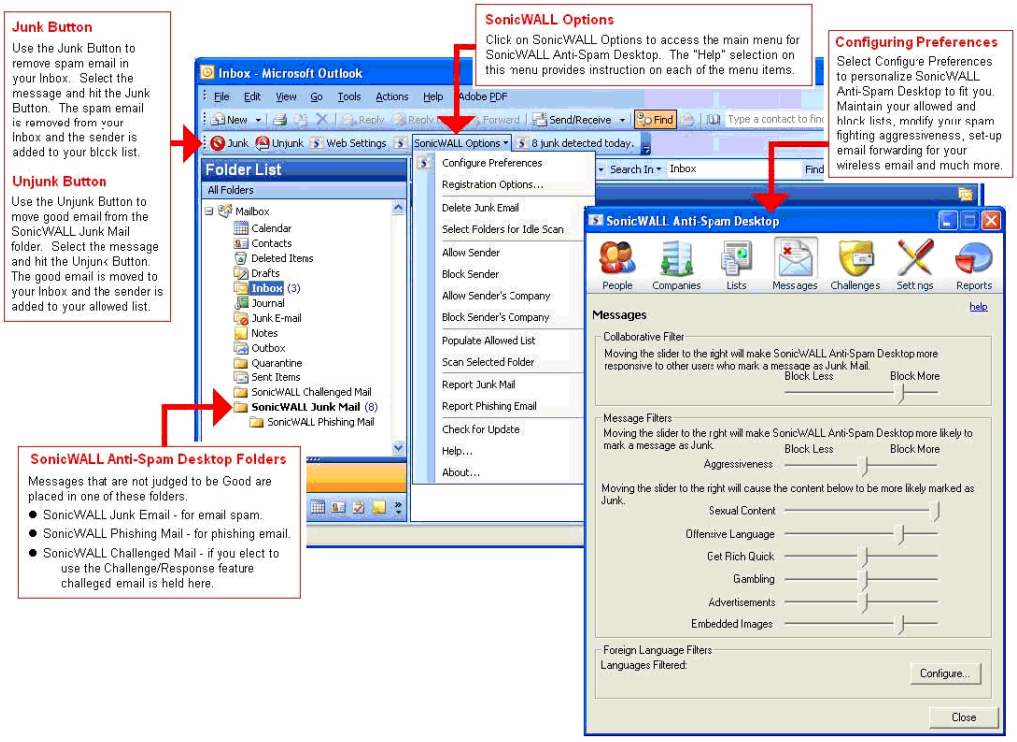
Using SonicWALL Anti-Spam Desktop

Using SonicWALL Anti-Spam Desktop is fast and easy. SonicWALL Anti-Spam Desktop protects your Inbox automatically. Once installed, you do not have to perform any configuration. Anti-Spam Desktop checks incoming messages, and automatically diverts junk mail to your SonicWALL Junk Mail folder based on your preferences.

SonicWALL Anti-Spam Desktop scans your outgoing mail to create a list of people with whom you want to exchange email. Those email addresses are placed on an Allowed List. SonicWALL does not scan email from people on the Allowed List.

SonicWALL is continuously gathering information on spam and other email threats. As new trends in email threats emerge, SonicWALL Anti-Spam Desktop is automatically updated.

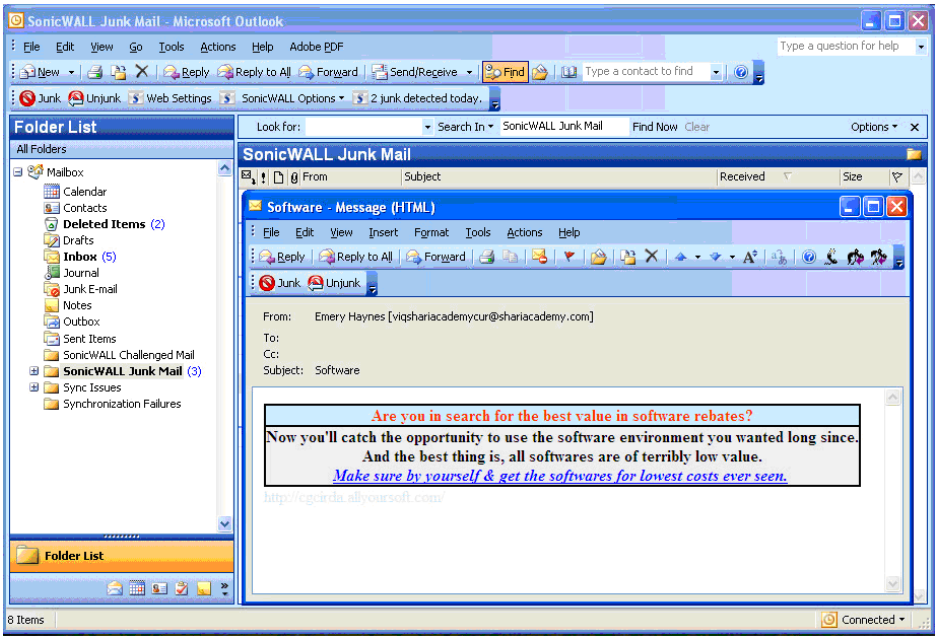
SonicWALL integrates into your mail client as follows:


Junk Button
Use the Junk Button to remove spam email in your Inbox. Select the message and hit the Junk Button. The spam email is removed from your Inbox and the sender is added to your block list.
Unjunk Button
Use the Unjunk Button to move good email from the SonicWALL Junk Mail folder. Select the message and hit the Unjunk Button. The good email is moved to your Inbox and the sender is added to your allowed list.
SonicWALL Options
Click on SonicWALL Options to access the main menu for SonicWALL Anti-Spam Desktop. The "Help" selection on this menu provides instruction on each of the menu items.
Configuring Preferences
Select Configure Preferences to personalize SonicWALL Anti-Spam Desktop to fit you. Maintain your allowed and block lists, modify your spam fighting aggressiveness, set-up email forwarding for your wireless email and much more.
Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help Adobe PDF
New Reply Reply Forward Send/Receive Find
Junk Unjunk Web Settings SonicWALL Options 8 junk detected today.
Folder List
All Folders
Mailbox
Calendar
Contacts
Deleted Items
Drafts
Inbox (3)
Journal
Junk E-mail
Notes
Outbox
Quarantine
Sent Items
SonicWALL Challenged Mail
SonicWALL Junk Mail (8)
SonicWALL Phishing Mail
Configure Preferences
Registration Options...
Delete Junk Email
Select Folders for Idle Scan
Allow Sender
Block Sender
Allow Sender's Company
Block Sender's Company
Populate Allowed List
Scan Selected Folder
Report Junk Mail
Report Phishing Email
Check for Update
Help...
About...
Search In Inbox Find
SonicWALL Anti-Spam Desktop
People Companies Lists Messages Challenges Settings Reports
help
Messages
Collaborative Filter
Moving the slider to the right will make SonicWALL Anti-Spam Desktop more responsive to other users who mark a message as Junk Mail.
Block Less Block More
Message Filters
Moving the slider to the right will make SonicWALL Anti-Spam Desktop more likely to mark a message as Junk.
Block Less Block More
Aggressiveness
Moving the slider to the right will cause the content below to be more likely marked as Junk.
Sexual Content
Offensive Language
Get Rich Quick
Gambling
Advertisements
Embedded Images
Foreign Language Filters
Languages Filtered:
Configure...
Close
SonicWALL Anti-Spam Desktop Folders
Messages that are not judged to be Good are placed in one of these folders.
SonicWALL Junk Email - for email spam.
SonicWALL Phishing Mail - for phishing email.
SonicWALL Challenged Mail - if you elect to use the Challenge/Response feature challeged email is held here.

When people send you email, SonicWALL Anti-Spam Desktop filters messages that contain spam and phishing, and prevents these messages from entering your inbox. SonicWALL Anti-Spam Desktop examines all incoming email and uses an arsenal of analysis techniques to determine if it is good mail or junk, including checking what other users think.

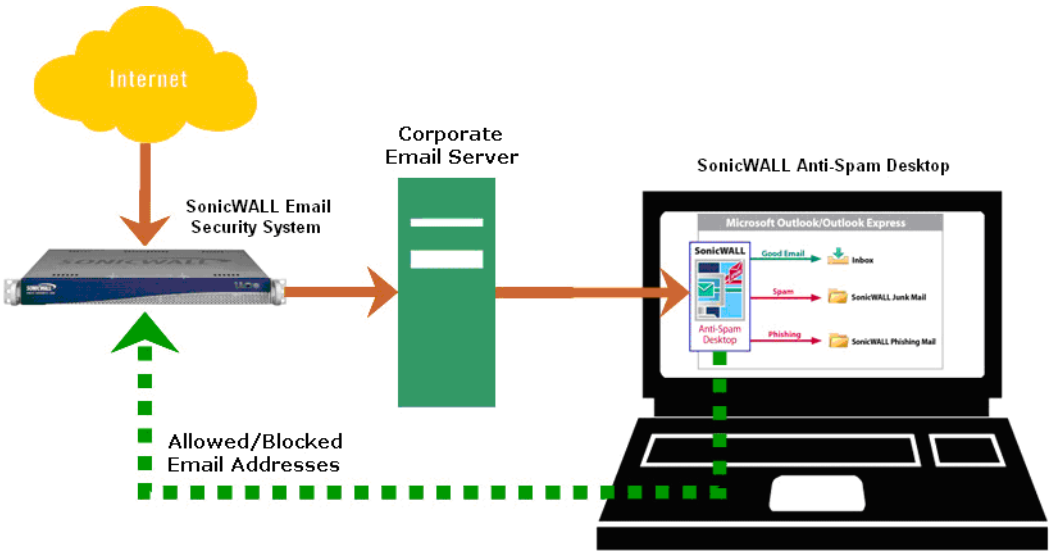
If SonicWALL Anti-Spam Desktop determines that incoming email is junk, the message is placed in the SonicWALL Junk Mail folder. SonicWALL Anti-Spam Desktop also analyzes email messages to determine if they are phishing. If they are, SonicWALL Anti-Spam Desktop puts these messages in the SonicWALL Phishing Mail folder. You can configure SonicWALL Anti-Spam Desktop to challenge questionable email messages. When you challenge an email message, SonicWALL Anti-Spam Desktop places it in the SonicWALL Challenged Mail folder, sends a message to the person who sent you the email, and waits for a response. If a response is received, the message is moved from the Challenged Mail folder to your Inbox and the sender is added to your Allowed List. If the mail is spam, the challenge will not receive a response because spam is mass-mailed. This email message will eventually be moved from the *Challenged* folder to your *Deleted* folder, based on your configuration preferences.

You can choose to open messages in the SonicWALL Junk Mail folder, SonicWALL Challenged Mail folder and SonicWALL Phishing folder and view these messages. If necessary, you can click **Unjunk** to move wanted messages in these SonicWALL folders to your Inbox. Here is an example of a Junk email message in a mail client:


SonicWALL Junk Mail - Microsoft Outlook
Folder List
SonicWALL Junk Mail
Software - Message (HTML)
From: Emery Haynes [viqshariacademycur@shariacademy.com]
To:
Cc:
Subject: Software
Are you in search for the best value in software rebates?
Now you'll catch the opportunity to use the software environment you wanted long since.
And the best thing is, all softwares are of terribly low value.
Make sure by yourself & get the softwares for lowest costs ever seen.

Integration with SonicWALL Email Security

If you use SonicWALL Anti-Spam Desktop in an environment that includes a SonicWALL Email Security gateway appliance or server-based software, Anti-Spam Desktop automatically integrates with the SonicWALL Email Security Solution. Here's how the SonicWALL Anti-Spam Desktop and SonicWALL Email Security solutions work together:



Configuring SonicWALL Anti-Spam Desktop

SonicWALL Options

Use the SonicWALL Options menu on the SonicWALL Anti-Spam Desktop browser toolbar to configure the Anti-Spam Desktop preferences.

Configure Preferences

Select **Configure Preferences** to display the SonicWALL Anti-Spam Desktop preferences window and configure the product to your needs, including options for viewing and updating Allowed and Blocked Lists, adjusting anti-spam settings, and more. Each of the configuration preferences screens has its own help link with assistance for that screen.

Registration Options

Click on **Registration Options...** to enter the valid License Key for your copy of SonicWALL Anti-Spam Desktop. Until you have entered a valid license key, the product is in Trial mode.

Delete Junk Email

Selecting Delete Junk Email will immediately move junk email from your SonicWALL Junk Mail folder and your SonicWALL Phishing Mail folder to your Deleted Items folder so they can be deleted by the system.

Select Folders For Idle Scan

The Idle Scan function scans the selected folders for newly identified spam and phishing email when your system is not busy. Decide which folders (if any) you wish to scan by selecting the *Select Folders* option, which will display the following window where you can place a check next to those email folders you wish to scan using the *Idle Scan* function.

Allow Sender

Select a specific email in the mail client. Then select this menu option to add the sender (the From: email address) of the selected email to the People Allowed List. If no email is selected, then nothing happens.

Block Sender

Select a specific email in the mail client. Then select this menu option to add the sender (the From: email address) of the selected email to the People Blocked List. If no email is selected, then nothing happens.

Allow Sender's Company

Select a specific email in the mail client. Then select this menu option to add the company name (domain name) of the From: email address of the selected email to the Company Allowed List. If no email is selected, then nothing happens.

Block Sender's Company

Select a specific email in the mail client. Then select this menu option to add the company name (domain name) of the From: email address of the selected email to the Company Blocked List. If no email is selected, then nothing happens.

Populate Allowed List

This option will scan your Sent email folder and add the receivers of each email to your People Allowed List.

Note:

- This can be done at installation time, but you can also skip this step at installation. If you have previously done this at installation time there is no need to do it again, although there is no harm in doing so.

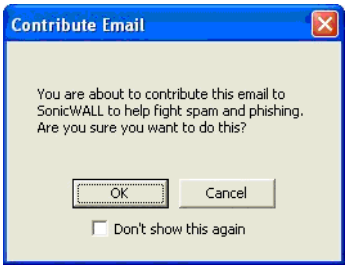
Scan Selected Folder

Select a specific email in the mail client. Then select this menu option to scan the selected folder and remove any identified spam and phishing email messages from that folder. If there are no folders containing email selected, then nothing will happen.

Report Junk Email

Select a specific email in the mail client. Selecting this menu option to send a copy of the selected email to SonicWALL for further analysis. Only use this option for those messages you believe are spam.

The first time (and possibly each time) you select this option the Contribute Email window asks you to confirm your desire to send the email to SonicWALL.


Contribute Email
You are about to contribute this email to SonicWALL to help fight spam and phishing. Are you sure you want to do this?
OK
Cancel
Don't show this again

The Contribute Email window will be displayed each time you select the **Report Junk Email** option unless you check the **Don't show this again** box and click **OK**. This double opt-in operation means that you will NOT be asked to confirm your subsequent submissions if you select the Report Junk Email menu option. To reset this option to its default setting, go to the SonicWALL Options > Configuration Preferences > Settings page and change the appropriate box in the Show Confirmations section.

Report Phishing Email

Select a specific email in the mail client. Selecting this menu option to send a copy of the selected email to SonicWALL for further analysis. You should only use this option if you believe the selected email is a phishing email.

The first time (and possibly each time) you select this option the Contribute Email window asks you to confirm your desire to send the email to SonicWALL.

The Contribute Email window is displayed each time you select the Report Phishing Email option unless you check the **Don't show this again** box and click **OK**. This double opt-in operation means that you will NOT be asked to confirm your subsequent submissions if you select the Report Phishing Email menu option. To reset this option to its default setting, go to the SonicWALL Options > Configuration Preferences > Settings page and change the appropriate box in the Show Confirmations section.

Check For Update

Use this option to use SonicWALL Anti-Spam Desktop to check with SonicWALL to see if there are any updates to the software available. SonicWALL Anti-Sam desktop automatically checks for updates on a regular basis, so you do not need this optionto keep your properly licensed software up to date.

SonicWALL Anti-Spam Desktop automatically checks for updates. If there is a new version of the software available, it attempts to download it from the SonicWALL datacenter and install it. This occurs in the background; you are notified when the update is complete.

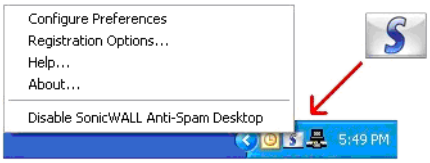
About

For information about the installation and operation of SonicWALL Anti-Spam Desktop, click **System Info**. The information displayed includes the product version, modules installed, your License Key, and the values of many of the SonicWALL Anti-Spam Desktop system variables.

To file a support request, click **Support**.

SonicWALL System Tray

The SonicWALL Anti-Spam Desktop icon appears in the System Tray on your Windows desktop. Right-click the icon to display the SonicWALL Anti-Spam Desktop menu:



Configure Preferences

Configure SonicWALL Anti-Spam Desktop as needed, including updating allowed and blocked lists, adjusting spam settings, and more.

Registration Options

Enter the valid License Key for your copy of SonicWALL Anti-Spam Desktop, select **Registration Options** from the Anti-Spam Desktop menu in the system tray. Until you have entered a valid license key, the product is in Trial mode.

About

For information related to the installation and operation of SonicWALL Anti-Spam Desktop, click **System Info**. The information displayed includes the product version, modules installed, your License Key and the value of many of the SonicWALL Anti-Spam Desktop system variables.

To file a support request, click **Support**.

Enabling and Disabling SonicWALL Anti-Spam Desktop

Click **Disable**, if it is available. A Restart window appears.

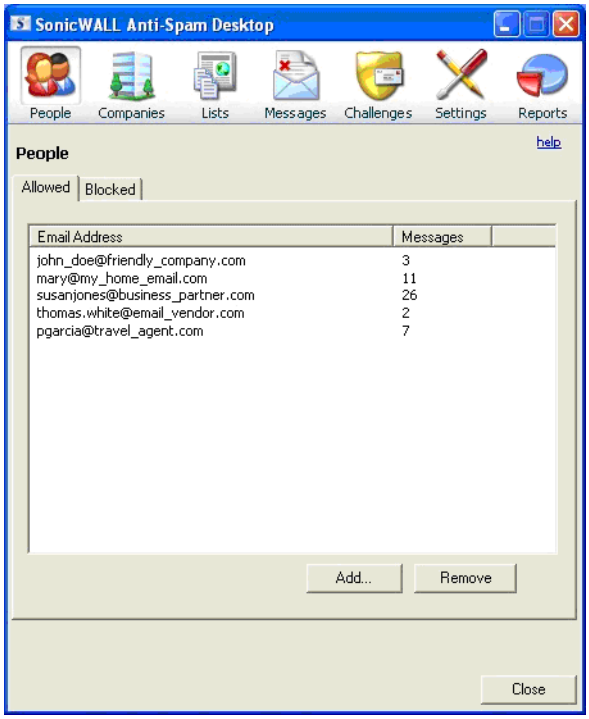
Click **OK**. SonicWALL Anti-Spam Desktop will be disabled when you exit Outlook or Outlook Express. If Outlook or Outlook Express is not running, disabling SonicWALL Anti-Spam Desktop will take place immediately.

The effect of disabling SonicWALL Anti-Spam Desktop means that it will no longer start when Outlook or Outlook Express is started and it will no longer filter email for spam or phishing. You must select *Enable* if you wish to reactivate SonicWALL Anti-Spam Desktop.

When you enable SonicWALL Anti-Spam Desktop it starts when Outlook or Outlook Express is started and begins filtering email messages for spam or phishing.

People

To see the lists of people who are allowed or blocked, click the **People** icon. Users can view the email addresses that have been added to each list, and add or remove items from each list as needed.



How the People Allowed List Works

When you add an email address to your People Allowed list, you are telling Anti-Spam Desktop that you want to always receive email from this email address. If Anti-Spam Desktop receives an email from someone on your People allowed list, the message is delivered to you even if Anti-Spam Desktop judges it to be spam or phishing.

There are different ways to add an email address to your People Allowed List:

- When you install Anti-Spam Desktop, the contacts in your default Contacts List are added to your People allowed list.
- When you send a message to someone, that person's email address is added to your allowed list. It is assumed that since messages are being sent to a specific address, the recipient is someone that you desire to receive correspondence from.
- Add email addresses manually to the Allowed list.

How the People Blocked List Works

When you add an email address to your People Blocked list, you are telling Anti-Spam Desktop that you always want to always block email sent to you from this email address. If Anti-Spam Desktop receives an email that is from someone on your People Blocked list, that email is placed in your Junk folder even if Anti-Spam Desktop judges the email to be good.

▶ **To add someone to the People Allowed list**

1. From the **People** window, click **Add**.
2. Enter a valid email address into the screen that comes up.
3. Click **OK**.

▶ **To remove someone from the People Allowed list**

1. From the **People** window, select the address you wish to remove.
2. Click **Remove**.
3. The email address is immediately removed from the list.

▶ **To add someone to the People Blocked list**

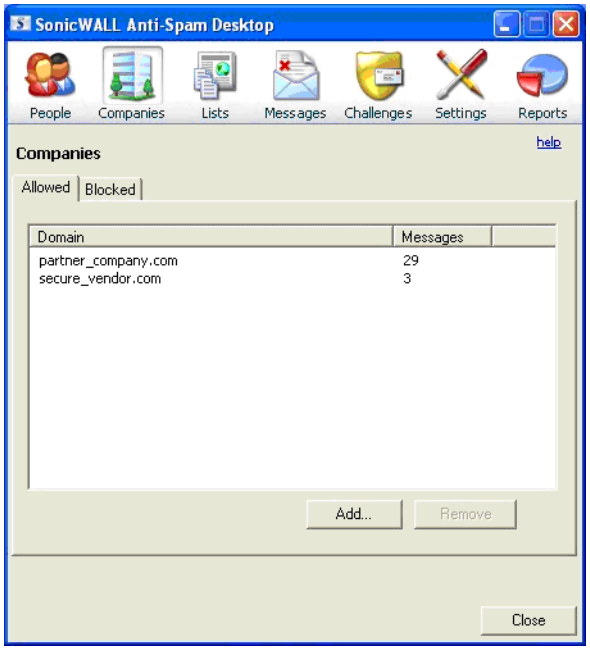
1. From the **People** window, click the **Block** Tab.
2. Click **Add**.
3. Enter a valid email address in the screen that comes up.
4. Click **OK**.

▶ **To remove someone from the People Blocked list**

1. From the **People** window, select the address you wish to remove.
2. Click **Remove**.
3. The email address is immediately removed from the list.

Companies

To see the lists of companies that are allowed or blocked, click the **Companies** icon. Anti-Spam Desktop assumes the domain (as in domain name) is the same as the company name. You can view the companies (domain names) that have been added to each list and add or remove entries as needed.



How the Companies Allowed List Works

When you add a company to your Companies Allowed list, you are telling Anti-Spam Desktop that you want to always receive email sent to you from anyone at that company. If Anti-Spam Desktop receives an email that is from anyone at a company listed on your Companies Allowed list that email will be delivered to you even if Anti-Spam Desktop judges the email to be spam or phishing.

Caution:

- Remember any email from anyone (real or fake) from a company listed in your Companies allowed list will be delivered to your Inbox.
- Spammers often spoof or fake the sending email address by using fake names of people at real companies - perhaps a company listed on your Companies Allowed list.
- Never add the name of your own company or your email ISP to the Companies Allowed list - spammers will often use your company name as the sender of the email.

How the Companies Blocked List Works

When you add a company to your list of companies that you want to block, you are telling SonicWALL Anti-Spam Desktop that you want to always block email sent to you from this company and anyone in this company. If Anti-Spam Desktop receives an email someone at a company on this list, the email is placed in your Junk folder, even if Anti-Spam Desktop judges the email to be good.

Your People Allowed list takes precedence over the Companies Blocked list. For example, if the email address *abc@example.com* is on your People Allowed list, but the company *example.com* is listed on your Companies Blocked list, you will receive the email.

▶ **To add a company to the Allowed list**

1. From the **Company** window, click **Add**.
2. Enter a valid company (domain) name in the screen that comes up.
3. Click **OK**.

▶ **To remove a company from the Allowed list**

1. From the **Company** window, select the company (domain) name you wish to remove.
2. Click **Remove**. The company name is immediately removed from the list.

▶ **To add a company to the Blocked list**

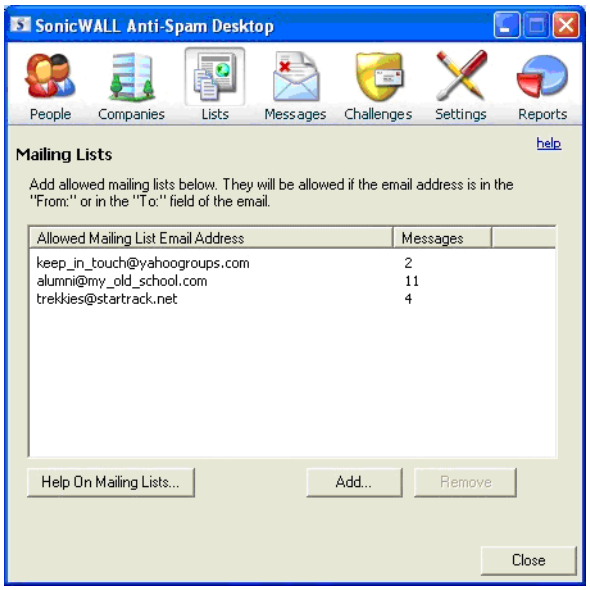
1. Click the **Block** tab.
2. Click **Add**.
3. Enter a valid company (domain) name in the screen that comes up.
4. Click **OK**.

▶ **To remove a company from the Blocked list**

1. Select the company (domain) name you wish to remove.
2. From the **Company** window, click **Remove**. The company name is immediately removed from the list.

Lists

To see the allowed mailing lists, click the **Lists** icon. You can view the email addresses that have been added to the allowed list and add or remove entries as desired.



How Lists Allowed Works

When you add an email address to your list of allowed mailing lists, you are telling Anti-Spam Desktop that you want to always receive email sent to you from this list. If Anti-Spam Desktop receives an email in which the From or To address is configured to be allowed, the email will be delivered to you even if Anti-Spam Desktop judges it to be spam or phishing.

Note

- Both the To and From email addresses are scanned to see if they match an entry in the Lists allowed list.
- An allowed email list can be overridden by an entry in the People blocked or Companies blocked lists. For example, if an email from a list named *myfriends@friendlist.com* is being junked, you may have inadvertently added the email address *myfriends@friendlist.com* to your People blocked list, or added *friendlist.com* to your Companies blocked list.

▶ **To add an entry to Lists Allowed**

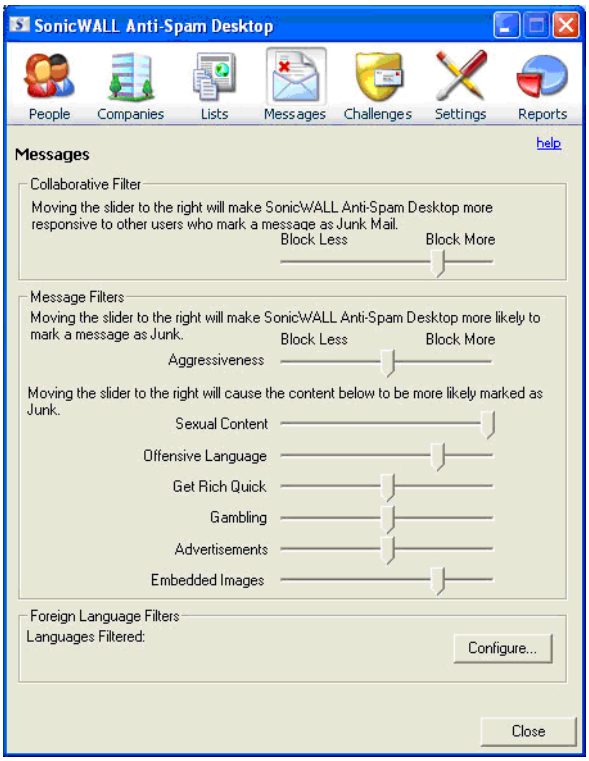
1. From the **Lists** window, click **Add**.
2. Enter a valid email address.
3. Click **OK**.

▶ **How to remove an entry from Lists Allowed**

1. From the **Lists** window, select the address you want to remove.
2. Click **Remove**. The email address is immediately removed from the list.

Messages

You can change the default settings for how aggressive you wish to be in identifying potential spam email that arrives in your Inbox. Click the **Messages** icon to configure settings for various filters.



Collaborative Filter

There are nearly 4 million people worldwide providing input into the Collaborative Filter - they are part of the SonicWALL Global Response Intelligent Defense (GRID) network. Movie the Collaborative slider to the right to make your system more responsive to the SonicWALL GRID and thereby block more messages. Move the Collaborative slider to the left to make your system less responsive to the SonicWALL GRID and thereby block fewer messages.

Messages Filter

Use the Messages Filter settings to control the aggressiveness of the included Adversarial Bayesian engine. The Aggressiveness Message Filter, the first slider bar in the Messages Filter section, sets overall aggressiveness. Moving this slider bar to the right will increase the number of messages considered junk by the system.

You can also fine-tune your aggressiveness based on the category of the message being evaluated. The categories are:

- Sexual Content
- Offensive Language
- Get Rich Quick
- Gambling
- Advertisements
- Embedded Images

If a message does not fall into one of these categories, Anti-Spam Desktop uses the Aggressiveness Message Filter settings as our guide. For each of the six different message categories, you can be more aggressive in blocking such messages by moving the appropriate slider bar to the right, or less aggressive by moving the appropriate slider bar to the left.

It is reasonable to have the slider bars in different positions of aggressiveness for each of the categories.

Foreign Language Filters

SonicWALL Anti-Spam Desktop allows you to block or receive messages that are written in various languages. The language is determined by examining the character set of each message received.

Select one of these options for each language:

- **Allow All**—Allows all messages using the character set for a given language to pass through the system and arrive in your Inbox, even if a given message is spam.
- **Block All**—Blocks all messages using the character set for a given language and places them in your junk folder, even if a given message is good.
- **No Opinion**—SonicWALL Anti-Spam Desktop evaluates the message and judges it junk or good.

Language Blocking and Allowed and Blocked Lists

Allowed and Blocked lists bypass language evaluation. For example, a message using the Korean character set from a sender on your People Allowed list is delivered to your Inbox even if you are blocking messages in Korean.

Challenges

Challenge / Response enables you to challenge none, some, or all email messages that arrive in your Inbox from unknown senders (someone who has not sent you email before). Set up your system to use the Challenge / Response capability if you want to challenge unknown senders.

How Challenge / Response Works

When Challenge / Response is set to All:

1. An email arrives to your system from an unknown sender.
2. If the message is judged to be spam or phishing it is placed in the appropriate *SonicWALL Junk Mail* or *SonicWALL Phishing Mail* folder and no further action is taken.
3. If the email is not judged to be spam or phishing it is placed in the *SonicWALL Challenged Mail* folder and the unknown sender is sent a Challenge email.
4. If a sender is real and responds to the challenge, he original email (which is being held in the *SonicWALL Challenged Mail* folder) is delivered to your Inbox and the sender is added to your People allowed list so that subsequent email messages from this sender will not be challenged.
5. If the sender does not successfully Respond to the challenge, the original email remains in the *SonicWALL Challenged Mail* folder where it can be deleted later. Unanswered challenge emails indicate automates sending or spamming.

Challenge / Response Levels

There are three different levels of Challenge / Response:

- **High - Challenge Unknown Senders**

  SonicWALL Anti-Spam Desktop challenges all email messages that you receive unless they are known as good to either you (on your allowed lists) or to SonicWALL (known good senders). Any email message that is received and can be classified immediately as junk gets sent directly to the SonicWALL Junk Mail folder for later deletion and does NOT get a challenge issued.

- **Low - Challenge Uncertain Email**

SonicWALL Anti-Spam Desktop only challenges email messages that it cannot determine with certainty are spam or are good. This is typically a small percentage of the email you receive.

- **Off - Never Send Challenges**

  SonicWALL Anti-Spam Desktop does not send challenge email messages. Move the slider up to turn on email challenges.

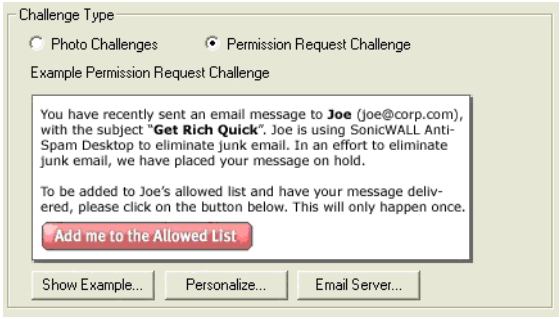
Challenge Type Entries and Buttons

Choose a Challenge Type to modify the challenge email sent out to the senders of challenged email messages.

Photo Challenge versus Permission Request Challenge

A Photo Challenge requires the person receiving the challenge to correctly select the number of items (in this case kittens) displayed in a picture:

The person receiving a Permission Request Challenge responds to the challenge by clicking **Add me to the Allowed List**.


Challenge Type
Photo Challenges
Permission Request Challenge
Example Permission Request Challenge
You have recently sent an email message to Joe (joe@corp.com), with the subject "Get Rich Quick". Joe is using SonicWALL Anti-Spam Desktop to eliminate junk email. In an effort to eliminate junk email, we have placed your message on hold.
To be added to Joe's allowed list and have your message delivered, please click on the button below. This will only happen once.
Add me to the Allowed List
Show Example...
Personalize...
Email Server...

Show Example Button

To see an example of the type of challenge message you can issue—Photo Challenge or Permission Request Challenge—click **Show Example**.

Personalize Button

To personalize your challenge message, click **Personalize**. The text you enter here is appended to the default challenge email (it does not replace it). The default message cannot be changed.

Email Server Button

Challenges are sent using the default SMTP server of your computer. If this is not configured correctly, or if more than one server is used to send out email, then there may be issues with the outgoing challenges. Use this option carefully and only if you need to specify a particular server.

▶ **Specify the SMTP server to use**

1. Enter the name of the SMTP server.
2. If required, select **My server requires authentication...**, then enter your login credentials (account name and password).
3. Click on **Send Test Email** to see if a message is sent from your system and arrives a few minutes later to your system.
4. Once you are certain your SMTP server is correctly configured, click **OK** to accept the new setup.

Settings

To configure Anti-Spam Desktop and optimize it for your deployment, click **Settings**.

Junk Folder Settings

Configure the length of time you store messages in the *SonicWALL Junk Mail* folder (including the *SonicWALL Phishing Mail* folder) and the *SonicWALL Challenged Mail* folder. To change these settings, click **Configure**.

Change the number of days that junk mail (spam and phishing mail) or challenged mail is kept before it is moved to your deleted items folder. The number entered must be a whole number and fall within the specified range for each folder: 1 to 10,000 days for junk mail and 7 to 10,000 days for challenged mail. The default is 30 days for both. Typical settings are 7 days for Junk Mail and 30 days for Challenged Mail. Keeping mail in the *Junk Mail* or *Challenged Mail* folders does not have an impact the performance of SonicWALL Anti-Spam Desktop.

Wireless Device Support (Email Forwarding)

You can set up your system to forward a copy of all good email to another valid email address, including, a Blackberry, Palm, iPhone and other PDA device.

▶ **To configure email forwarding**

1. Click **Configure** in the **Wireless Device Support** section.
2. Enter the email address to which the message will be forwarded. Remember that this can be any device with a valid email address. Anti-Spam Desktop forwards all good email messages to this address. More than one email address can be entered; separate multiple entries with a space.
3. If you want to forward just the message headers, and not the whole message, click **Next**.
4. Enter the maximum number of email messages (or headers) that should be forwarded in any 24-hour period.
5. Click **Email Server** if you need to configure the outgoing SMTP server. This is only necessary if you are not using the default SMTP server to forward your email. You may need to discuss this setting with your email system administrator to determine if a value is needed here and what that value should be. Once you have set up this option click **Send Test Email** to determine if it is working correctly.

Notes

- The email forwarding feature within SonicWALL Anti-Spam Desktop does not work if the email application is not open / accessible (that is, if you are not logged in to your email account). This means that the client system that is forwarding your email must be operational and receiving email so that it can be forwarded.

- Messages cannot be forwarded through the SMTP server if it requires authentication and no authentication is configured, or if the authentication is not configured correctly or has changed. Verify that your SMTP settings are correct.
- Only the email messages are forwarded, not attachments. The original email with any attachment remains on the client system after a copy is forwarded.
- The **Forward Email Headers Only** option may be useful if any of the following is true:
  - If you are forwarding email to a device that shows only a small amount of data
  - You do not wish to use up expensive bandwidth by forwarding the entire email
  - You want to be notified only of new messages

Auto-Report Phishing Email

To send phishing email you receive to SonicWALL for analysis, select this option. This helps us ensure that phishing email is correctly identified and removed from your Inbox.

The first time a phishing email is detected and queued to be sent to SonicWALL for analysis, you are prompted to confirm that you want this email sent. Email sent from your system using this option is placed in your Outbox and sent like any other email.

Show Confirmations

When you select **Report Junk Mail** or **Report Phishing Email** from the SonicWALL Options menu, you can opt to see a confirmation window. For example, if you select **Contribute Junk Email** a confirmation window appears when you select *Report Junk Mail* from the SonicWALL Options menu.

This gives you complete control over the email messages that are leaving your system, even if they are junk or phishing messages.

Outlook Multiple Inbox Support

By default, SonicWALL Anti-Spam Desktop scans only the default Outlook Mailbox for spam and phishing messages. To scan inbox messages for other IMAP or POP3 accounts or Exchange mailboxes, select **Outlook Multiple Inbox Support**. This setting applies only to Outlook.

Rescan Folder

You can have your Inbox rescanned for spam or phishing email. This enables the system to remove junk email from your Inbox based on the latest information received from the SonicWALL GRID.

You can specify how often you wish to rescan your Inbox and how many days to go back in the rescan process. The rescan is only done when the system is idle so that it does not interfere with your use of the computer system.

SonicWALL Anti-Spam Desktop Signature

Select this option to place the following signature block at the bottom of all email you send (it appears only if you are not using another default signature):

```
This mailbox protected from junk email by SonicWALL Anti-Spam Desktop from
SonicWALL, Inc. http://www.sonicwall.com.
```

Note

- The SonicWALL signature block is automatically inserted when the application is in trial mode. When the application is purchased and converted to a registered version, the signature block is deactivated.

SonicWALL Notifications

To be alerted regarding new, highly aggressive, spam and phishing threats, select **SonicWALL Notifications**. A popup window appears in the lower-right corner of your screen when new threats are discovered.

Note

- When you receive a notification such as this, be aware that this is a general warning issued to everyone in the SonicWALL Anti-Spam Desktop community: it does not necessarily mean that you have been exposed to this particular type of spam or phishing email.

Reports

To view a given report, click the **Reports** icon and go to the corresponding tab:

- **Junk by Day**—Uses a bar chart representation of the last 5 days worth of email received overlaid with the last 5 days of junk mail received.
- **Reasons**—Uses a bar chart representation to illustrate the methods used to identify junk mail for the current week.
- **Total History**—Uses a line graph representation to illustrate the total number of email received versus the total number of junk email received over the past 300 days. Due to the amount of data being analyzed, the display of this report can take several seconds.
- **Total Reasons**—Uses a bar chart representation to illustrate the methods used to identify junk email messages since the installation of the application.

Troubleshooting

- How can I tell if SonicWALL Anti-Spam Desktop is working?

  There are three things to check to verify SonicWALL Anti-Spam Desktop is operational.

  - Is SonicWALL Anti-Spam Desktop launching correctly when you open Outlook or Outlook Express?

    You should see the SonicWALL Anti-Spam Desktop toolbar with the **Junk** and **Unjunk** buttons visible.

  - Are you still getting spam in your inbox?

    SonicWALL Anti-Spam Desktop should make an immediate impact to reduce the amount of spam that you receive in your inbox.

  - All junk email filtered out by SonicWALL Anti-Spam Desktop is sent to one of three folders. Check these folders to see if there is any junk email:

    SonicWALL Junk Mail folder
    SonicWALL Phishing Mail folder (within the SonicWALL Junk Mail folder)
    SonicWALL Challenged Mail folder

- What happens when I use Outlook, Outlook Express, or Windows Mail rules?

  Most of the time, SonicWALL Anti-Spam Desktop processes before rules are processed. This is the expected behavior. However, under certain conditions (such as low memory), rules may be processed first. This is because your mail client loads first and begins processing before the SonicWALL Anti-Spam Desktop plug-in is loaded.

- Can I have other anti-spam products installed with SonicWALL Anti-Spam Desktop?

  SonicWALL Anti-Spam Desktop may not operate correctly when installed on a machine that already has an installation of a different anti-spam solution. Both products will be competing for mail client resources, which can result in neither product operating properly. SonicWALL recommends uninstalling other anti-spam products before installing the SonicWALL Anti-Spam Desktop.

- I have Microsoft Junk Email protection. Do I need SonicWALL Anti-Spam Desktop?

  The decision is up to you. SonicWALL Anti-Spam Desktop has features such as Anti-Spam Aggressiveness Settings, Foreign Language Blocking, SonicWALL GRID Network Updates, Challenge/Response, Bayesian Phishing Engine, a separate Phishing Folder, and more. These features are not part of the Microsoft Junk Email protection product.

- Can SonicWALL Anti-Spam Desktop be used with Microsoft Junk Email Protection?

  Yes, but the results can be confusing. For example, SonicWALL delivers spam it detects to the *SonicWALL Junk E-mail* folder and Microsoft delivers spam it detects to the *Junk E-Mail* folder, creating two different places for spam to reside. In addition, both systems attempt to keep

Allowed and Blocked lists that are not shared. If you are going to use SonicWALL Anti-Spam Desktop, we recommend that you turn off Microsoft Junk Email Protection.

- How do I uninstall SonicWALL Anti-Spam Desktop?

  You can uninstall SonicWALL Anti-Spam Desktop from the Windows Start menu or Control Panel.

▶ **To uninstall from the Start Menu**

1. Close down any open programs, including your mail client.
2. Click **Start** and select **All Programs**.
3. Select **SonicWALL Anti-Spam Desktop**.
4. Click **Uninstall**.
5. Click **Next**, and then click **Finish**.

▶ **To uninstall from the Control Panel**

1. Close down any open programs, including your mail client.
2. Click **Start**, and select **Control Panel**.
3. Double-click **Add or Remove Programs**.
4. Select SonicWALL Anti-Spam Desktop, then click **Change/Remove** to start the uninstall.
5. Click **Next**, and then click **Finish**.

SonicWALL, Inc.
2001 Logic Drive
San Jose CA 95124-3452
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

PN: 232-001812-00 Rev A

©2009 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.